AU/ACSC/COLE/AY09

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

DEVELOPING CAPABILITY: THE USE OF LASER COMMUNICATION TECHNOLOGY TO OPERATE IN A CYBER-DENIED ENVIRONMENT

by

Patrick E. Cole, LCDR, USN

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Lieutenant Colonel Michael P. Linschoten

Maxwell Air Force Base, Alabama

April 2009

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
APR 2009	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Developing Capability: The Use of Laser Communication Technology to Operate in a Cyber-Denied Environment	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Air Command And Staff College Air University Maxwell Air Force Base, Alabama**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

US forces rely heavily upon various systems in order to navigate, communicate, employ weapons, synchronize data links, and transfer a wide variety of data. Nearly all battlefield systems rely upon some form of electronic technology to function and can be hindered in one way or another. Geography, atmospherics, bandwidth, intentional and unintentional interference, and jamming can range from tolerable annoyance to complete compromise. The basic capability to freely and securely navigate and communicate on the battlefield is essential to enable strategic, operational and tactical objectives. Laser technology may hold the key to reliable and sustainable navigation and communication capability options in a cyber-denied environment. In a problem solution research methodology, the examination of strategies, directives and doctrine will be used to demonstrate the need to maintain and continuously develop the technologies providing this capability. Recent examples of advanced technology use by potential adversaries will be utilized to demonstrate the acuity of current and future threats. Current civilian and military technologies will be examined in order to provide the reader with exposure to the existing capabilities and limitations. To respond to current and anticipate future needs, current and in-process civilian and military laser technologies will be examined in order to expose their employment capabilities and limitations, reflecting the need to further develop such technologies to provide the warfighter with the basic capability to navigate and communicate in the complex and uncertain cyber-denied battle-space of current and future conflicts.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**SAR**	**45**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

Disclaimer

The views expressed in this academic research paper are those of the author(s) and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Contents

Illustrations

Preface

After several deployments as a carrier-based command and control platform pilot, nothing has frustrated me more than not being able to navigate from 'A' to 'B,' and not being able to verbally or digitally (and securely) communicate freely with someone at any distance. These frustrations were often the result of electromagnetic interference, faults and/or differences in equipment, line-of-sight issues, satellite availability, or enemy jamming and subversion capabilities. If one couples demonstrations of anti-satellite technologies, computer hacking, and enemy advances in tactics, techniques and procedures with our increasing reliance upon the latest and developing technologies to operate, our forces require the technology to communicate and navigate freely now, and in the future. As an aviator, I hold very dear the basic ability to freely aviate, navigate and communicate, verbally and digitally, in the current and increasingly complex future battle-space of the air, land, sea, space and cyber domains.

I would very much like to thank Lt Col Mike Linschoten and Lt Col Mark Black for their incredible guidance and support in focusing my energy to this project's fruition. Their direction of the Air Command and Staff College (ACSC) 'Warfare in The Cyberspace Domain' Research Elective sparked analytic and critical thinking nodes I did not know I possessed. I would like to thank fellow ACSC students Maj Paul Williams and Maj Robert Bridges for their invaluable insights and perspectives from previous USAF communication and space assignments. A very special thanks to Maj Jason Schmidt, Assistant Professor of Electro-Optics at the Air Force Institute of Technology, whose subject matter expertise and knowledge of existing and future laser technology projects was of great importance. All of the above gentlemen eagerly provided me with the data, insight and alternate ways of problem thinking that allowed me to synthesize a research paper that could positively influence current and future battlefield operations. *Thanks!*

Abstract

US forces rely heavily upon various systems in order to navigate, communicate, employ weapons, synchronize data links, and transfer a wide variety of data. Nearly all battlefield systems rely upon some form of electronic technology to function and can be hindered in one way or another. Geography, atmospherics, bandwidth, intentional and unintentional interference, and jamming can range from tolerable annoyance to complete compromise. The basic capability to freely and securely navigate and communicate on the battlefield is essential to enable strategic, operational and tactical objectives. Laser technology may hold the key to reliable and sustainable navigation and communication capability options in a cyber-denied environment.

In a problem solution research methodology, the examination of strategies, directives and doctrine will be used to demonstrate the need to maintain and continuously develop the technologies providing this capability. Recent examples of advanced technology use by potential adversaries will be utilized to demonstrate the acuity of current and future threats. Current civilian and military technologies will be examined in order to provide the reader with exposure to the existing capabilities and limitations. To respond to current and anticipate future needs, current and in-process civilian and military laser technologies will be examined in order to expose their employment capabilities and limitations, reflecting the need to further develop such technologies to provide the warfighter with the basic capability to navigate and communicate in the complex and uncertain cyber-denied battle-space of current and future conflicts.

Introduction

Man did not create the land, did not create the sea, did not create the air, nor did he create space. Over many hundreds of years, forces have attempted to control all or various pieces of each of these four domains throughout the many great battles of history. Strategic objectives in past and current conflicts have included attaining air, land and/or maritime superiority. As technology continues to leap forward, space superiority will only increase in importance. In addition, the race for advanced technology among the nations of the globe puts a fifth domain, *one man did create*, up for grabs. This fifth domain is what is termed as cyberspace, and it is equally important. Cyberspace transcends the four existing domains, and can both help and hinder supremacy in all five domains.

It thus follows that cyberspace supremacy will enable the nation, state, or non-state actor the capability to move freely through air, land, sea, and/or space as appropriate to the conflict at hand. Since the ability to move involves the ability to navigate and communicate, to include the verbal and digital realms, he who understands that cyberspace is intrinsic to the air, land, sea and space domains comprehends that coherent and synchronized control of this man-made domain is critical to his or her ability to conduct operations while simultaneously denying the enemy their ability to do the same.

In this modern age and in ages to come, the thirst for technology has fueled the desires of the armed forces of the world for capabilities to execute precision operations globally. Technological advances provide the warfighter capability to produce effects that range from the simple to the broad, the simple to the highly complex, and from large scale to pin-point accuracies. The ability to drop a GPS-guided weapon within a five foot radius of accuracy exists. The ability to neutralize communications through jamming or internally from ‘crashing’ a

cellular telephone company server exists. Even more alarming, are the abilities to disrupt satellite operations through dazzling, and/or destroying satellites in low earth orbit (LEO) with an earth-launched weapon. While many of these abilities are currently possible by only those with the scientific knowledge and necessary infrastructure, low-tech abilities should also not be neglected, nor should the United States discount non-state actors obtaining such capabilities.

The attacks of 11 September 2001 reflected a moderate level of technology (a commercial aircraft and its operation) and infrastructure intrusion (entry into the United States, knowledge of FAA procedures) to disrupt day-to-day civilian, commercial and military activities on American soil. Forces in Iraq and Afghanistan continue to combat electromagnetic interference (EMI), line-of-sight (LOS) and jamming/disruption obstacles, along with other enemy technological innovations, in order to conduct effective operations. China, among its capabilities to conduct a wide variety of cyber operations, demonstrated the ability to use anti-satellite weapons. North Korea is rumored to be developing similar capabilities. Cyber attacks have occurred in Estonia. Recently, much debate and re-organization of USAF Cyber Command has happened, along with discussions among the other Services' cyber divisions regarding roles and responsibilities. As time elapses, enemy capabilities and TTP's continue to evolve, be theorized about, and either revealed or discovered. As a capable nation, the United States must continue its quest for technology to anticipate and respond to the applications of potential enemy cyber capabilities.

Throughout history, technology has attributed positive and negative qualities to the battlefield and the mode and speed in which forces communicate, navigate and operate. The advent of rifled cannon, land- and sea-based aircraft, the nuclear weapon, Special Operations Forces, stealth technology, and real-time datalink/communications systems linking the battlefield

soldier or UAV to a computer thousands of miles away, each have had their contributions. The ways in which new technologies have been utilized on the battlefield have shaped the current conflict and fostered friendly and enemy innovation in the uses of current and developing technologies for future battles. If the armed forces are to learn valuable lessons from which to adapt to coming conflicts, we must understand the situation, enhance flexibility to the situation, and anticipate future needs by developing and providing the capability for air, land, sea and space forces to operate effectively in view of the race for technology.

The concept that as time elapses, technology progresses, and friendly and enemy armed services develop capabilities reflects that US forces in the battlefield will face a real, robust, adaptable and capable threat that could deny US forces the ability to attain air, land, space and/or maritime superiority. It follows thus, in order for US forces to ensure operations can be sustainable, alternate capabilities to communicate (voice and data) and navigate in a cyber-denied arena must be developed. This need is evident in the ever-growing omnipresence of current and future threats. The basic requisite to aviate, navigate and communicate must be met. We must explore new technologies in to fly, fight and win in cyberspace. We cannot wait until potential adversaries have the capability to deny our freedom of action in cyberspace. As US forces rely heavily upon various systems in order to navigate, communicate, employ weapons, synchronize data links and transfer a variety of data, developing laser communication technologies could provide the capability to execute and sustain navigation, transmission of data and verbal communications in a cyber-denied environment.

Why The Need?

Guidance & Doctrine

Guidance and direction are directly reflective of an organization's purpose. In any organization, guidance and direction usually filters from the top down, and the organization then responds with capabilities and limitations in the form of its operational doctrine. When doctrine is inadequate, doctrine is adapted or created anew. When new means of warfare are developed, doctrine is adapted or modified to translate the new developments into a warfighter's edge on the battlefield. At its foundation, guidance, direction and doctrine originate from a need to anticipate, and if needed, respond to a threat through posture or direct projection of power. In the context of the Department of Defense (DOD), senior leaders such as the Joint Chiefs of Staff (JCS), Secretary of Defense (SECDEF) and Combatant Commanders (COCOMs), contribute and work to enact Presidential (POTUS) strategic guidance.

This strategic guidance is filtered down from the strategic and operational levels to the tactical level through vetted documents such as the National Security Strategy of the United States (NSS), the National Military Strategy of the United States of America (NMS), the Quadrennial Defense Review (QDR), and the National Strategy to Secure Cyberspace (NSSC). Strategic guidance reaches the tactical warfighter in doctrine such as Air Force Doctrine Documents (AFFDs), Naval Warfare Publications (NWPs) and Tactical Manuals (TACMANs), Army Field Manuals (FMs), and Joint Publications (JPs), among others. It is from this framework that capabilities are developed in order to utilize current technology, as well as adapted or created in order to integrate new technologies.

The March 2006 NSS states "We have seen great accomplishments, confronted new challenges, and refined our approach as conditions changed."[3] It also states, in terms of weapons

of mass destruction (WMD), "The new strategic environment requires new approaches to deterrence and defense. Our deterrence strategy no longer rests primarily on the grim premise of inflicting devastating consequences ... Both offenses and defenses are necessary to deter state and non-state actors, through denial of the objectives of their attacks and, if necessary, responding with overwhelming force."[4] In addition, the NSS references the 2006 QDR in which the DOD will "… continue to adapt and build to meet new challenges … **traditional** challenges …" and "… **disruptive** challenges from state and non-state actors who employ technologies and capabilities (such as … cyber and space operations, or directed energy weapons) in new ways to counter military advantages … [emphasis in original]."[5]

The 2006 QDR goes on to note how forces are continually changing, "… [by] integrating new technologies …" and "… investing in new equipment, technology and platforms."[6] To do so,

> "The United States will develop capabilities that would present any adversary with complex and multidimensional challenges and complicate its offensive planning efforts. These include the pursuit of investments that capitalize on … key strategic and operational areas, such as persistent surveillance and long-range strike, stealth, operational maneuver and sustainment of land, sea and ground forces at strategic distances, air dominance and undersea warfare. These capabilities should preserve U.S. freedom of action and provide future Presidents with an expanded set of options to address … focus areas and a wide range of potential future contingencies … to possess sufficient capability to convince any potential adversary that it cannot prevail in a conflict …" These capabilities include "persistent surveillance … that can penetrate and loiter in denied or contested areas" … "Secure broadband communications into denied or contested areas to support penetrating surveillance and strike systems" … "air dominance capabilities to defeat advanced threats" … "Capabilities to shape and defend cyberspace" … and … "Joint command and control capabilities that are survivable in the face of WMD-, electronic-, or cyber-attacks."[7]

Along the same venues of new approaches to deterrence and defense of the NSS and the QDR to adapt and build to meet traditional and disruptive challenges, the 2004 NMS describes the "the ways and means to … **prevail** against adversaries who threaten … deployed forces, allies and friends [emphasis in original]."[8] To do so, a "capabilities-based approach" is required that "uses operating concepts … to guide the development of warfighting capabilities."[9] These

new capabilities-based approaches are required because "Adversaries threaten … throughout a complex battle-space … spanning the global commons of international airspace, waters, space and cyberspace."[10]

For the US to apply force, it "requires power projection assets to move capabilities rapidly, employ them precisely and sustain them even when adversaries employ anti-access and counter power projection strategies … Effective global strike … results from a combination of precision and maneuver and the integration of new technologies, doctrine and organizations … The armed forces must have the ability to operate across the air, land, sea space and cyberspace domains of the battle-space … [to include the ability to counter] threats in cyberspace aimed at networks and data critical to US information-enabled systems."[11] Similar guidance is put forth in the NSSC. Under NSSC Priority V, the US faces enemies "who could launch cyber attacks or seek to exploit our systems … In wartime or crisis, adversaries may … attempt to slow the US military response by disrupting systems of the Department of Defense …"[12]

At the tactical level, volumes of doctrine exist from the various Services. As a specific example that carries similarly through other doctrine, Joint Publication (JP) 3-01 *Countering Air and Missile Threats*, captures the strategic guidance to provide persistent offensive and defensive air capabilities. It directly supports the direction, stating a capability requirement for a,

> "C2 [Command and Control] system … able to seamlessly flow information and warnings and to control assets from one mission/task to another, based on the daily requirements to support the JFC's [Joint Force Commander's] operation/campaign. Communications architecture is a critical element for counterair due to the time sensitivity of some targets. The C2 system must connect sensors to intelligence nodes and decisionmakers, and to operate throughout the operational area."[13]

To summarize, strategic guidance, direction and doctrine put forth a great many challenges in this technologically driven age. The armed forces must meet these challenges head

on and not only adapt to the current situation, but be adaptable and flexible in anticipating future needs. They must also pay strict adherence to the role the adversary will play. As the strategies put forth, and the next chapter will expand upon, the adversary also has a similar technological drive and a willingness to use it. The adversary's drive will not only foster the strength of their forces, but develop the capabilities to counter, deny and/or exploit friendly technology. To address these issues, the necessary technology has to be developed, integrated and trained to a high level of proficiency.

To fly, fight and win in all five warfare domains, developing and integrating advanced technologies enable the capabilities to freely navigate and communicate in the battle-space. The need for a military that can support friendly national objectives is vital to the global position of the United States. The direction that filters down to the Services tasks them with providing the capable arms of military power to support the diplomatic, economic and informational objectives of the nation when called upon. Without the technology to at least put up a fair fight in cyberspace, the Services will face a steep uphill climb in the fight for air, land, sea and space superiority, a task that strategic guidance from the top has filtered down to the warfighter.

Why The Need?

Threats

From the previous section, the guidance filtered down through the strategic, operational and tactical levels reflected the preparation of armed forces capabilities to respond to threats to the United States. As put forth in the national strategies, these responses require continuous updates as new challenges are introduced to the battle-space, to include the utilization of new technologies that provide an edge on the battlefield. However, it is not just the United States with a technological thirst. This nation and its military forces have witnessed enemy uses of advanced technology in both military and non-military actions. Let us examine a few recent examples of enemy demonstrations and consider how these episodes either directly or indirectly could be used to, attack, exploit or deny US forces freedom of navigation and communication. These examples directly reflect the need for advanced technological development.

China's Use of Technology

On 11 January 2007, China's third attempt to demonstrate capability to use a kinetic anti-satellite (ASAT) weapon succeeded.[14] According to CJCS Marine Corps General Peter Pace in a 28 May 2007 report, "It wasn't clear what [China's] intent was, and when things are not clear and when there are surprises, it tends to confuse people and raise suspicions."[15] Since it was China's third attempt, in contrast to General Pace's remarks, the event probably should not really have been a surprise. In a tacit response, the US demonstrated the same capability in February 2008 when the USS Lake Erie launched an SM-3 missile to intercept and destroy a US satellite travelling at more than 17,000MPH.[16] However, it should be pointed out China's race for this and other technological means has been an ongoing process for an unknown amount of time. What China intends to do with the technology may, however, come as a surprise.

Andrew Scobell, referencing the 1995-1996 Taiwan Straits controversy, advocates "the principle of active defense … has been at the core of Chinese strategic thinking for decades, [and] does not preclude offense."[17] Others who have studied China's history have similar insights. Timothy Thomas points out, "… the PLA [People's Liberation Army] has invested a great amount of time in finding a way to utilize EMP [Electromagnetic Pulse] devices to neutralize the digital devices of the [US Navy's] 7th Fleet if the latter decided to intervene in any potential conflict between Taiwan and China … [and] investing in C4ISR [Command, Control, Computers, Communications, Intelligence, Surveillance and Reconnaissance] technology to ensure they can protect their digital systems in space and potentially cause harm to an opponent's C4ISR capability.[18]

Leigh Armistead broadens the horizon of China's potential, stating "… the current commitment of the Chinese armed forces to high-tech based warfare … may be at a very primitive level compared to the US armed forces, but they are writing doctrine and experimenting with IO [Information Operations] on a constant basis."[19] Timothy Thomas also reflects the high-tech aspect of China's active defense in writing "Attacks should be directed against nodes that sustain the enemy's war system and against weak points that are hard to replace or regenerate and results in unstoppable chaos … One must destroy the enemy's brain and central nervous system … through attacks against structures and procedures of the enemy's operational systems … Information systems and support systems must always be the first targets and then the stronger weapons systems."[20] China is not a lone actor in demonstrating capabilities posing threats to US forces, as shown by events in Estonia, Iraq and Afghanistan.

Estonia, Georgia, Iraq, Afghanistan & Beyond

In what some may contend was the first cyber war, Estonia experienced a crippling

distributed denial of service (DDoS) attack. From the end of April to mid-May, the attack on Estonia "came close to shutting down the country's infrastructure, clogging the Web sites of the president, the prime minister, Parliament and other government agencies, staggering Estonia's biggest bank and overwhelming the sites of several daily newspapers … the hackers infiltrated computers around the world … to perform these incursions. The computers [became] unwitting foot soldiers …"[21] While the attackers' identity may never be known, the attacks on Estonia demonstrate a threat capability that could bring a military organization or nation to its knees, much in the same way China would symbolically go after the enemy's brain and nervous system.

"In recent years, cyberattacks have been associated with Middle East and Serbian-Croatian conflicts. But computer systems at the Pentagon, NASA, universities and research labs have been compromised in the past."[22] The August 2008 Russian invasion of Georgia reflected similar veins of the Estonia attack, attacking the media, banking and the Ministry of Foreign Affairs, but also coordinated this action with invasion by military forces.[23] It is not beyond reason to believe these DDoS and other forms of cyberattacks could be formed against US military organizations at home and abroad, threatening military freedom of action, as will be explored in the next section.

In the cases of Iraq and Afghanistan, US military forces have had to contend with a broad range of enemy threats to freedom of action. The area geography and population centers already contribute to the high levels of electromagnetic interference (EMI) in Iraq, degrading communication systems to greater and lesser degrees, coupled with some line-of-sight (LOS) range limitations common to radio sets experienced in Afghanistan. All over the commercial media and in military channels, improvised explosive devices (IEDs) are a frequent headline, their detonation often triggered by cellular phones, automotive/garage door remotes and other

hand-held electronic devices. Global Positioning System (GPS) jamming was experienced in Iraq, and the heavy reliance by US forces upon GPS based systems strengthens the need to protect GPS integrity as the sophistication of jammers increases and cost of ownership decreases.[24] Such jamming devices may become key factors in future battles as nations such as China, the Former Soviet Union and North Korea continue to develop new means to deny GPS.[25]

To summarize, senior leaders have recognized US forces needs and provided the strategic guidance to the chain of command. The chain of command has responded and must continue to respond with tools that enable doctrine to be executed in the battle-space. If potential enemies are ignored, their capabilities will threaten friendly force ability to verbally and digitally communicate, navigate and employ weapons. Without the technology to do so, the enemy has the potential to compromise GPS navigation and weapon employment, and deny or disrupt radio, telephone and computer communication systems. Such an enemy could potentially deny or disrupt the entire computer-based logistics system, the data-link communications required to execute the time intensive and verbal- and data-fed mission of Airborne Battlefield Command and Control (ABCC), or the control feed of unmanned aerial vehicles (UAVs).

In addition, the effects of denying intelligence, surveillance and response (ISR) platforms the ability to transmit time-critical data, would result in complete chaos at the Operations Centers. The need for the capabilities advanced technologies can provide is real. Without these capabilities, the warfighter will be without direction, and battle-space commanders will be without the information and tools required to keep pace with the adversary. In short, the US will lose and lose badly if the needs are not adequate to face the high-tech adversary.

Dependencies, Capabilities & Limitations

For commanders and warfighters at the strategic, operational and tactical levels, the ability to observe and act upon a common operating picture (COP) and command and control the battle-space are high priority capabilities. The intake and exhaust of information and the speed of transmittal is critical to timely decision making. Friendly and enemy forces can win or lose a fight in the blink of an eye in today's high-tech chain of command. Be it a forward air controller on the ground utilizing unmanned aerial vehicle (UAV) video for CAS,[26] an airborne or sea-based air controller sending prosecution commands to fighter aircraft, a bomber aircraft entering target data into a GPS-guided weapon, the Combined Air Operations Center (CAOC) Commander transmitting approval to attack a target via secure satellite radio, or a logistician entering movement data details into Surface Deployment and Distribution Command (SDDC) systems, the military of today's world has an un-extractable dependency upon technology. However, in view of enemy strategies and demonstrations of the possible ability to attack, deny or exploit these types of critical systems, the modern warfighter must be aware of the limitations and vulnerabilities of these critical systems, and how enemy attack could compromise navigation and communication on the battle-space.

For military air, land, ground, sea and space forces, very high frequency (VHF), ultra high frequency (UHF), high frequency (HF), frequency modulation (FM), and satellite (SAT) radios and associated cryptographic equipment constitute the primary 'normal' means of battle-space communication. Data links such as Link-16 and Cooperative Engagement Capability (CEC) augment, and in some cases supersede, these normal radio systems providing a means to share sensor data composing a COP or single integrated air picture (SIAP), to include fire control solution quality data. These data links also are capable of transmitting items such as imagery,

live UAV video, web-based information, and command and control execution commands, with or without additional verbal communications. Consequently, the joint tactical air controller (JTAC) can use UAV remote operated video enhanced receiver (ROVER) feed to observe enemy activity and guide CAS aircraft to the target, in addition to passing entire attack requests with few verbal transmissions. ABCC platforms with COP situational awareness can provide targeting priority and engagement direction to fighter aircraft with merely a click of a button, rather than verbally.

VHF, UHF, HF and FM radio sets are subject to EMI, LOS, jamming and intrusion by the enemy, as well as saturation by own forces, as seen in Iraq and Afghanistan. Satellite radio sets are affected by these issues to some degree, but their limited available uplink and downlink channels, as well as antenna and space vehicle cones of visibility, often result in unavailability or lack of discernable transmissions. Military aircraft operating in Iraq frequently encounter EMI issues, and those in Afghanistan encounter LOS issues, requiring C2 aircraft to act as relays for communication, taking away resources from the mission at hand. Those familiar with Arabian Gulf operations know aircraft experience frequent and distracting queries from non-US entities.

In terms of cryptographic technologies, Have-Quick (HQ) and devices such as KY-57's and KY-58's provide layers of protection for radio systems. These types of devices work to ensure security of radio transmissions against jamming and information compromise through frequency-hopping (HQ) and the encoding of audio tones (KY). While they do add layers of security in protecting information, their transmissions are still subject to the EMI, LOS and (in small part) jamming limitations by the enemy. While there has not been any proven intrusion of data link systems or normal radio cryptography, it should not be assumed their complex means of operation will never be broken by the enemy's push for technology discussed previously.

In addition to the radio issues, the reliance upon GPS is also of critical concern as technology progresses. GPS today can be found in almost every type of navigation and communication device. Manned and unmanned air, land, sea and space forces alike rely heavily upon GPS for navigation, friendly and enemy unit tracking, radio and data link synchronization and weapons employment. The commercial airline industry has increased the sensitivity of aircraft navigation technology to more densely populate the airways in the form of reduced vertical separation minimums (RVSM). Older forms of navigation aids such as VHF Omni-directional Radio Range (VOR) and TACtical Air Navigation (TACAN) are slowly disappearing, in favor of GPS precision. In more and more systems, GPS time is the baseline time used to synchronize data links such as Link-16 and CEC, among others. GPS-guided weapons are becoming, if not already, *the* weapons of choice in the modern fight in order to decrease circular-error probable (CEP), minimize collateral damage estimates (CDE) and achieve the effects of hard-target penetration munitions. And in other industries, GPS is used to track items ranging from semi-trucks, to pets, to individual packages.

Galileo In-Orbit Validation Element-A (GIOVE-A), a venture of the European Union, European Space Agency and private investors, is Europe's version of US GPS.[27] "Members of Cornell's GPS Laboratory were able to crack the so-called pseudorandom number (PRN) codes [of the satellite]."[28] While the cracking of the GIOVE-A PRN codes gives users access to the GPS data, it is not beyond comprehension to suggest that other similar types of efforts might lead to the loss of GPS data, control of GPS satellites, or the intrusion of malicious code to the GPS system. In the recent past, forces in Iraq witnessed the use of and destroyed several Russian and Chinese made GPS jammers.[29] At the most extreme, the use of ASAT weapons could remove the GPS element of navigation and communication completely.

To summarize this section, we cannot rest on our laurels that current technologies will be forever secure and we must develop capabilities that ensure future freedom of action. The dependencies US forces rely upon to bring capability to the battle-space are not without their limitations. Some of these limitations are the result of the devices themselves, the platform in which they are installed and/or the area of operations (AOR). Other 'limitations' are those the enemy will seek to employ through attack, denial or exploitation. Enemy thirst for technology fuels their capabilities to do such things as the cyber attacks of Estonia and Georgia, jam GPS and radio units in Iraq and Afghanistan, broadcast UAV video on the internet, and monitor our supply and troop movements. In the future, it is safe to assume their technological and employment capabilities will only grow stronger and more difficult to counter.

Similar fuel must be applied to protect and provide US military force freedom of action capabilities today that take into account our current dependencies and limitations, and anticipate those of the future. This un-extractable dependency on technology requires normal radio and satellite communications, GPS for navigation, time synchronization and weapons employment, and the integrity and security of sustained access to these systems. The enemy will look to attack, deny and exploit the dependencies upon and limitations of US systems to their advantage. US freedom of action on the battle-space could be drawn to its knees without the means to rely upon the capabilities of the systems which we are so dependent. Without being able to securely communicate, perform logistics, execute C2, employ GPS weapons, and provide a COP/SIAP to Force Commanders, the lack of advanced technology will be a critical limiting factor that hands the battle-space edge to the enemy.

Laser Technologies

The laser, or Light Amplification by the Stimulated Emission of Radiation, has been in existence in various forms since the late 1950's. At a very basic level, lasers produce light through the organized stimulation of an atom to produce the release of photons to encounter the electrons of another atom that has the same excited state.[30] The cascading effect that occurs results in many photons of the same wavelength and phase that release energy.[31] Depending on the atom used, the wavelength of the laser may fall across a broad range of frequencies in the electronic spectrum.[32] The beauty of lasers is that they contain one specific wavelength, are coherent and are very directional.[33] These three particular characteristics of lasers make them ideal for high-bandwidth usage and have greater security than traditional radio transmissions.

In general, the radio spectrum shown at the bottom of Figure 1, spans from ~3 kilohertz (kHz) to 300 gigahertz (gHz), covering the upper end of very low frequency (VLF) to the extremely high frequency (EHF) radio transmissions.[34] As shown in the exploded view of the radio spectrum in Figure 1, the RF spectrum has been organized to provide for countless numbers of agencies and applications. Similar division of military specific AOR frequencies occurs for the various military agencies/units, designating certain channels/frequencies for items such as C2 agencies, aerial refueling operations, JTAC coordination, and ISR assets. Even with these divisions, the frequencies designated for military operations can be jammed, degraded by LOS or EMI, or simply be overloaded with units passing routine or high-priority, time-critical information, ranging from a post-mission in-flight-report to requests for immediate fire when troops are in close enemy contact. These frequencies can also suffer from degradation from airframe interference and the dust, dirt and grime of the operating environment upon radio equipment components.

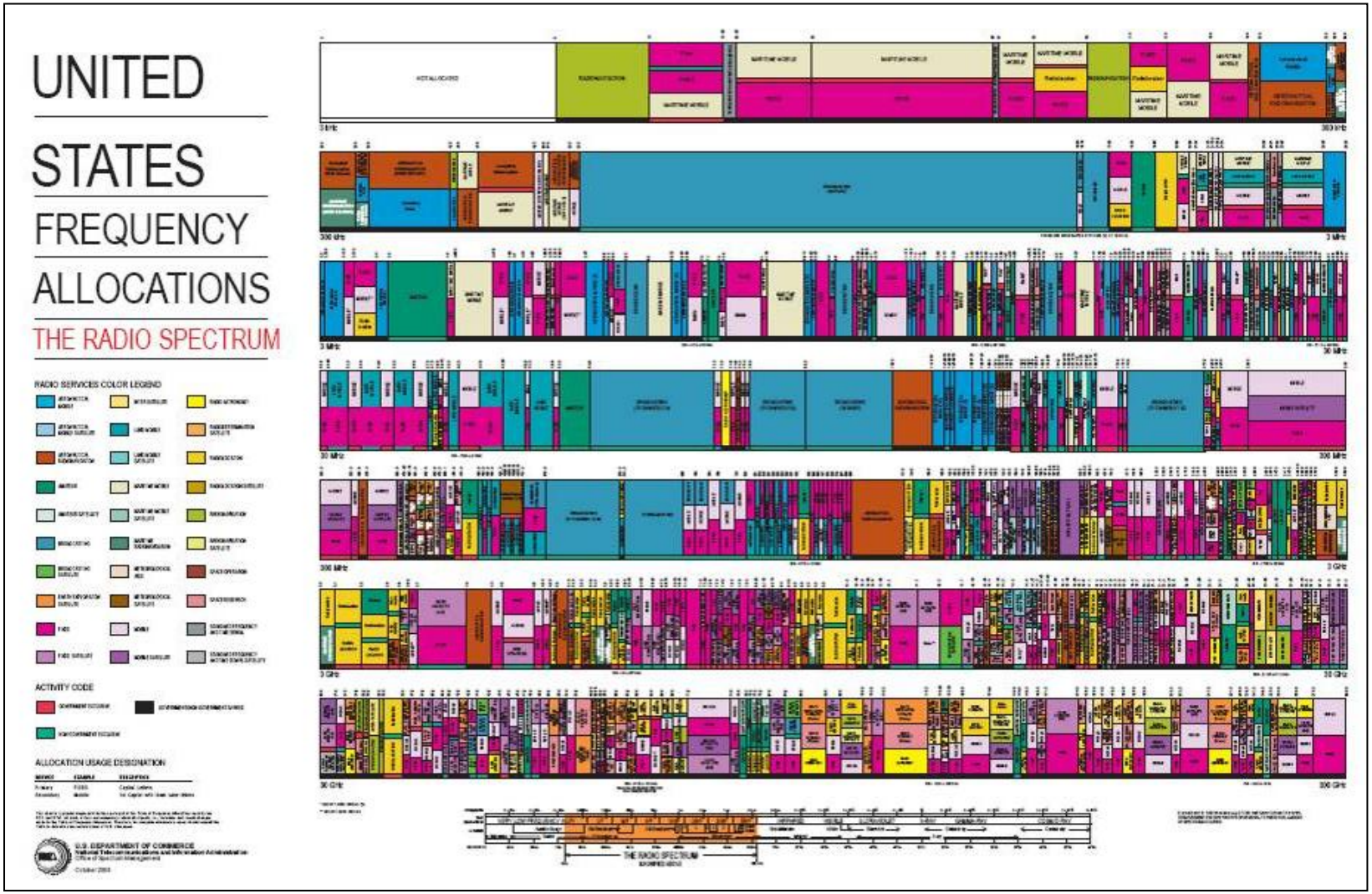

Figure 1: United States Frequency Allocations[35]

In contrast to traditional radio frequencies, laser technology uses frequencies in the infrared (IR), visible and ultraviolet (UV) ranges (among others depending on type), as well as those of the 'L' (UHF) and 'C' super high frequency (SHF) traditional bands.[36] The other great asset of laser technology is the vastly larger amount of data that can be transmitted, with estimates ranging from 10 gigabits per second to 100 terabits per second depending on application.[37] Various military and non-military agencies have developed technology and experiments to expose the advantages of lasers, many of them having initial beginnings related to space. For example, the Defense Technical Information Center (DTIC) has a 1989 Massachusetts Institute of Technology/Lincoln Laboratory (MIT/LL) technical report that details a concept of a free-space optical communication (FSOC) system for space use.[38]

In 2004, Space News reported on a 5-watt laser NASA intends to use to transfer large amounts of data collected by space vehicles, with a planned launch of the satellite orbiter this year (2009).[39] This satellite, the Mars Telecommunications Orbiter, would allow for the downloading of "… bandwidth-intensive imagery and other data collected by planetary orbiters, probes and landers."[40] Two years after this report, Boeing in conjunction with MIT/LL, sponsored by the Military Satellite Communications (MILSATCOM) Joint Program Office and National Reconnaissance Office (NRO), was able to show "… the MILSATCOM user community that it can have a 10 to 40 gigabit per second TSAT [Transformational Satellite Communications System] backbone. In the decades ahead, laser communications will be a key technology and an enabler for missions of vital importance to US security and major element of the US Department of Defense's vision for TSAT."[41]

In non-space domains, laser technology has shown potential as well. In 2004, Bell Labs and Lucent technologies were awarded multi-million dollar US DOD contracts to research and

develop the Coherent Communications Imaging and Targeting (CCIT) program, and the Integrated Router Interconnected Spectrally (IRIS) program.[42] These programs are to demonstrate "high-speed and long-range laser communications", and the "next generation of super-fast, ultra-high capacity optical communications."[43] Sea-based forces are also active in research and development of laser-based communication and data systems. The Naval Research Laboratory (NRL) has been testing ship-mounted laser communication for evaluation, and similar research has been proposed for submarine and Special Forces interaction by the Naval Undersea Warfare Center (NUWC).[44]

As two last examples, the US Defense Advanced Research Projects Agency (DARPA) has been experimenting with LADAR (laser detection and ranging), to "permit reconnaissance and combat aircraft to detect and identify ground targets more rapidly and efficiently than with radar."[45] Lastly, AOptix Technologies has already produced the LCT-5 Lasercomm Terminal, with laser technology that is "able to simultaneously and seamlessly provide communications for both manned and unmanned airborne and ground systems and installations throughout the battlespace … a strategic and tactical network, linking airborne assets, tasking, processing, exploitation and dissemination centers and ground-based 'On the Move/At the Halt' (OTM/ATH), dismounted and maneuver-force elements."[46]

As demonstrated by the examples, much of the laser technology and its currently known advantages are being researched and developed, and show great promise for military applications. However, the technology still has distance to travel to become an asset throughout the battle-space. As many of the examples have pointed out, lasers have difficulty with atmospheric turbulence, water droplets, haze, heavy cloud cover and aircraft vibration.[47] In addition, the current levels of development are only at the initial stages of discerning how to

perform signal acquisition, and point and track laser-based non-space systems.[48] Even so, it is reasonable to expect that these issues will be resolved through the progress of technology.

With the current and possible future levels of laser technology, what might a battle-space presentation of a laser based verbal and digital communication and navigation system conceptually look like? Figure 2, from Hamid Hammati's 2003 Jet Propulsion Lab (JPL) presentation, reveals a good place to start.[49] Figure 2 shows laser technology used to relay UAV imagery of a ground event via satellite to fixed and mobile ground stations. The large data transfer capability of lasers, coupled with LADAR and such things as night-vision technology would allow for extremely detailed, secure (with additional cryptographic equipment if needed), full motion video ISR of a particular combat area under almost any condition and time of day. Expanding to a larger scale, now add fighters, bombers, warships, ISR and C2 platforms. These units, with the increased data stream of lasers, would now have a much larger situational awareness of the air, land and sea domains and the ability to make more informed and timely decisions based on friendly and enemy disposition, not to exclude the vast increase of information available to theater/CAOC commanders. Users of datalinks would find much more information at their fingertips and its update rate would be much, much higher.

In addition to the increases in imagery and data flow, add the laser communications aspect. Relieved from the constraints of jammed and/or transmission-clogged traditional radio sets, operators would now have pinpoint, directed, more secure (encrypted if necessary) means to communicate not only imagery, but also other data and verbal transmissions, leaving the enemy unaware they are even happening. As another advantage, ground, sea and air platforms equipped to interact with a laser-based system could also be able to refine their position and movement, much in the same way GPS-aided inertial navigation systems (INSs) and hand/vehicle-mounted

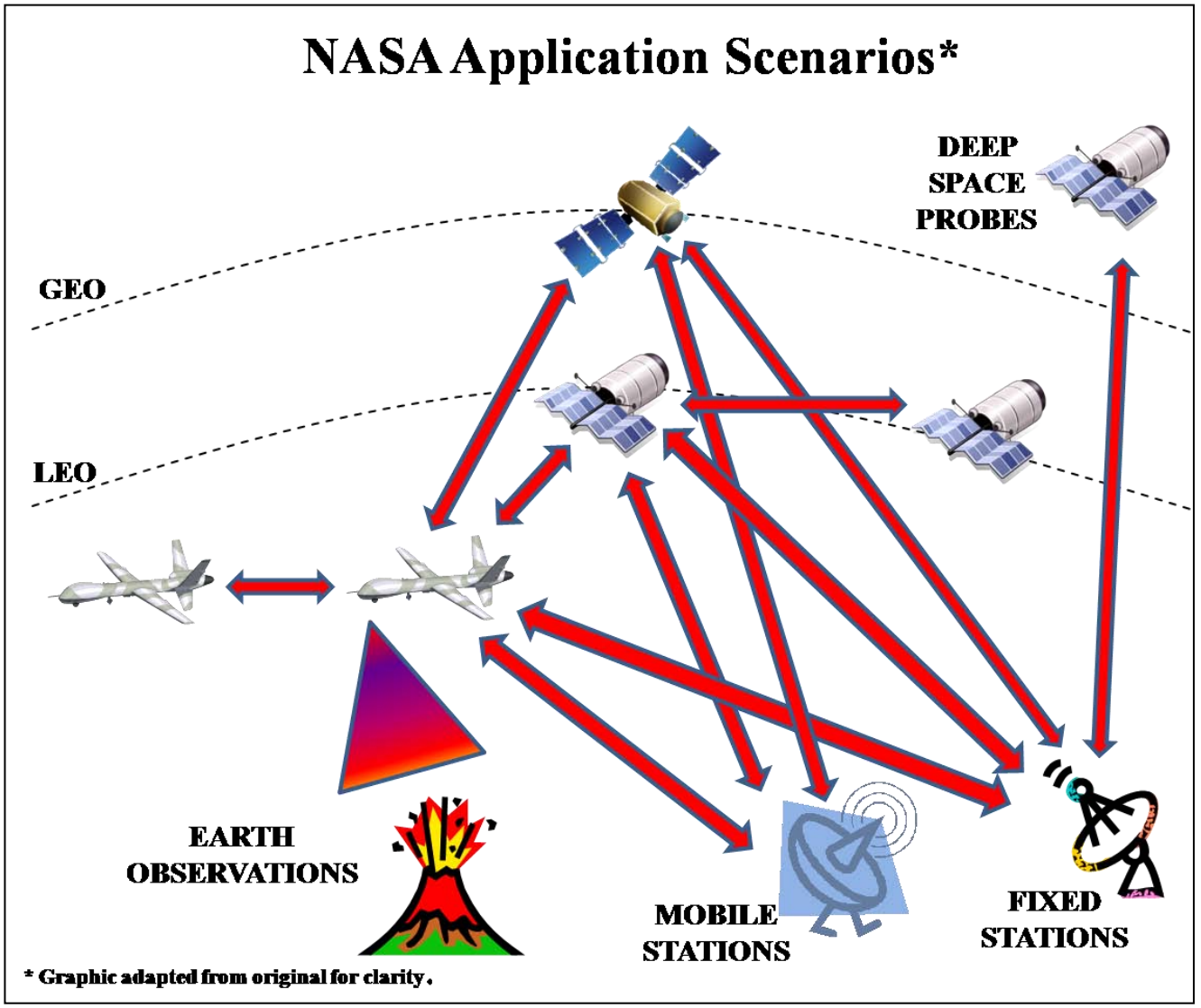

Figure 2: NASA Application Scenarios[50]

GPS systems currently perform, potentially without needing a GPS signal. This could also include the control of UAV platforms and other remotely operated systems.

To deploy the system (or use as an everyday system), aircraft, ships, ground equipment and radio and datalink devices will require modifications to interact with laser-based systems. Existing satellites and new satellites in low- or geo-stational earth orbit will require devices for connectivity. Ground and sea-based units may need additional antennas or tethered balloons to extend range, such as a modified Tethered Aerostat Radar System (TARS) developed by the USAF and the National Oceanic and Atmospheric Administration (NOAA).[51] Various areas of a theater may require the placement of antennas or TARS-type devices in order to provide coverage and extend range. These devices may need to be placed by special forces (SOF) or air-dropped from combat logistics aircraft. Depending on the technology, these devices could be small enough to be deployed by tactial aircraft in the same manner as chaff/flare ejector systems. In addition, these devices may not need to be more than a 'beacon' similar to those for aerial navigational, which would provide a means for orientation and time synchronization for entry into datalink-type systems from distant sources, such as a friendly nation or aircraft carrier at sea.

Deploying such a system in full or in part may or may not come about from enemy activities. The system might be deployed at the onset of military involvement as a result of the intelligence preparation of the battle-space, or at a theater commander's direction. Or it may be required to deploy as a result of enemy forces completely or selectively denying or exploiting traditional navigation (such as GPS) and communication (VHF, UHF, etc.) systems. These systems might also operate in a burst-type mode, making enemy denial, exploitation or intrusion attacks extremely difficult and ensuring friendly freedom of action in navigation, weapon employment and verbal and non-verbal communications.

Laser Technology Drawbacks

There are numerous issues requiring an intense effort and need to draw upon the knowledge and experience of those already immersed in this area for laser technologies to enhance military freedom of action. Opponents of laser technological research, development and utilization could argue the hill of technology advancement is just too steep to climb. The current level of development of laser technology will need to increase. The feasibility and means of employment and inherent limitations will require a large amount of planning for its use. Training air, land, sea, space and cyber forces and the maintenance personnel on these systems will add to time-to-train. Doctrine will need to be updated, and high-level commanders will require education of the options and perhaps additional security clearance levels for access. Aircraft, ships, spacecraft and ground equipment will need to be modified to incorporate the new equipment, to include the time and process of test and evaluation. The associated costs may outweigh the benefits. The military, commercial and civilian industries just do not have the technology and development processes in place that are required. Lastly, which service should take the lead in driving the need through all these obstacles could result in a significant lead time before work even begins.

As reflected by the previous section, laser technology has great potential. Lasers have been in existence for decades, but their use for communication and navigation has really only taken off in the recent past. Applications already exist for the space program, as do uses for ground forces such as range finders for GPS weapon targeting and laser designating devices for laser guided weapons. Small scale, short range laser modems can be built relatively cheaply for data transmission.[52] However, the state of laser technology has not yet reached the point where full scale, theater wide military use is a reality.

Though lasers can be operated in a very directed, narrow and short beam, and carry large amounts of data in very small packages, lasers still operate on a frequency and are subject to interference problems over long distances, especially through the atmosphere. Frequencies are also subject to attack through jamming and intrusion, as well as EMI and LOS problems. The dirty and rough environment where conflicts have occurred and where forces operate may detract from, damage and/or incapacitate sending and receiving devices. The directed, narrow and short transmission characteristics of lasers may counter some of these problems, but it is not yet known to what extent and how well. Frequency hopping and other cryptography equipment may also aid in protecting the transmissions, but the complexity of these systems may diffuse the ability to transmit the data. In addition, the means of navigation systems to interpret the incoming data and correct for errors in pointing, tracking and atmospherics have not been fully developed, which could result in the loss of position and time reference for other communication, navigation and weapons systems.

As with the technological gap, how to employ such a technology has a long road to travel. The means to deploy and employ the system will require an intense planning effort by commanders, the intelligence community and operators alike to decide where and when the system were to be put in place via such means as rockets into LEO, free-floating or tethered balloons, air drop, ground troops, or Special Forces, among other still undeveloped means. Coupled with the technological gap, the equipment itself may or may not contain sensitive equipment US forces would not want in enemy hands. Considerations also have to made such as: How long does the system last? Is it battery or solar powered? Are there means to automatically or remotely zeroize any sensitive equipment and data? For devices such as balloons and satellites, is the system 'disposable' enough that once the conflict is over, or a

device is captured by the enemy, that it is not cost-preventative and compromising to friendly forces in order to just let the lost or captured device go? How would it be deconflicted from other units operating in its vicinity? These questions also lead to other issues opponents could argue against laser technology, such as training and doctrine.

In addition to the above, the time-to-train of US forces would be extended by the need to familiarize air, land, sea and space forces, to include maintenance personnel in laser technology use. Implementation would require additional training assets, to include facilities, and personnel. Manuals and publication for forces and maintainers alike will be required, to include the legwork needed for additional operational doctrine such a TTP's and FM's. These items will not only require the manpower to create, but also the time to develop and field throughout the forces' various training pipelines, as well as increased time-to-train. At the higher levels, commanders will require knowledge of the capabilities and possibly the clearances to discuss and employ this and related capabilities in the battle-space. The 'jointness' of today and the future might be the most at risk, as non-US forces may not have the equipment, training and proficiency required to utilize such a system.

Even if the technology, ways to deploy and employ, and knowledge of the capability fully existed, the modification of the tools of war to use a laser-based system will take time and money. The test and evaluation process of prototype equipment will take months, if not years to make its way to the warfighter, as it does with any 'new' military product. Once past test and evaluation, the modification of existing aircraft, ships, spacecraft and ground equipment will inevitably take an equal amount of time, as well including the resources needed in the military parts supply system. And as mentioned earlier about doctrine, the various service weapons schools will require anywhere from a few months to a few years to work with the technology and

modified platforms in order to provide the warfighter with the tactics, techniques and procedures to use the platforms to our advantage.

Overall, the financial and manpower costs involved may outweigh the benefits, but two of the biggest obstacles may be pushback from industry and the leadership of the endeavor. In general, it is safe to state that a business exists today to make money. Large businesses, particularly those that work on government issues, bid on projects to produce a product and make a profit. It could very well occur that the business or group of businesses that wins the contract to produce such a laser based system does not produce a product that meets expectations, or the project gets bogged down in legal disputes between partner businesses, as seen in the past with various weapons and aircraft manufacturers. In addition, the question as to which of the services will take ownership of the project may fall into dispute and result in inter-service rivalries, extending a possible rollout of such as system, as seen in the many discussions and re-organizations surrounding a 'cyber' command.

To summarize, there are many stout challenges to the role laser technology could play for the warfighter. Costs and leadership/ownership may be the strongest points an opponent might argue, but there are equal challenges and unknowns about laser technology that need to be fully vetted in order to prove its worth. In view of all of these challenges, it must not be overlooked that the strategic, operational and tactical warfighter requires capabilities, and will require additional capabilities in the future, to ensure freedom of action in the *battlefield* that has become a highly complex, multidimensional and trans-dimensional *battle-space*. It is this fifth dimension, cyberspace, that transcends the air, land, sea and space, that opponents to laser technology must give credit to and allow for all levels of warfighter to have freedom of action.

Conclusion

So what? Why should we consider laser communications technology as an area to research and develop capabilities for the warfighter? Should we not be concerned about what laser technologies could provide in a cyber-denied environment, an environment in which our current communication, navigation and precision weapons systems employment capabilities could be in jeopardy, and in the future, even the security of cryptographic equipment could be compromised? Should we not be concerned about the health of the Global Information Grid (GIG) and not be concerned about attempting to protect the integrity of systems we may not even know are being intruded (such as the enemy listening in on traditional radio and data systems)? The answer, if we are to learn from history but not be enrapt by it, and anticipate the future in light of potential adversary technological advances, is a definitive and emphatic *no*. We must be concerned about threats potential adversaries pose and anticipate those it will pose tomorrow by developing what laser-based communication technology can bring to the warfighter.

On 29 September 2008, the Vice Chairman of the Joint Chiefs of Staff, released a memorandum with a definition of cyberspace operations:

> "The employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid."[53]

This definition eats at the heart of the technologically-reliant force we have become. In order to achieve objectives and produce effects, US forces must have freedom of action in the form of capabilities. In view of the threats enemies have demonstrated discussed earlier, and in anticipating those of the future, the vision that is required is one that must challenge the current levels of technology to new heights to provide for the warfighters at all levels: "The Department's [DOD] vision is to develop cyberspace capability that provides global situational

awareness of cyberspace, US freedom of action in cyberspace, the ability to provide warfighting effects within and through cyberspace, and, when called upon, provide cyberspace support to civilian authorities."[54]

The security and high-bandwidth advantages laser communication could potentially provide would enable the technologically-reliant US forces to ensure freedom of action. Commanders and operators could have the timely information needed to make strategic, operational and tactical decisions resulting in the efficient and effective execution of operations, while helping to ensure the safety and security of forces. Providing for the needs of our forces now will aid in combating 'technology creep.' Just as expensive and sometimes military only technology has filtered down to street-corner availability, such as GPS, satellite imagery ('google maps') and lasers (CD/DVD players), we must be prepared for other advanced technology to eventually filter down from large nations to smaller nations, non-state actors and rogue organizations that could potentially threaten US force freedom of action.

Laser communication technology may be one of the many pathways to freedom of action. Its assets, and those yet to be uncovered through research, development and testing, may very well give the warfighter the edge required to support the strategic objectives promulgated from POTUS and reflected in service doctrine. While it may take time to incorporate the advantages laser technology can provide, understand its capabilities and limitations, adapt or write new doctrine to utilize it, and train and equip forces to use it, the enemy should not be discounted as doing the same. The China of the 1950's in the Korean conflict arose from an extremely limited technological base to build aircraft and missiles, submarines and ships of enormous capability, in some cases better and in some cases worse than current US force capabilities. They have clearly learned their lessons from history and made leaps and bounds in technological advancement and

utilization to pose a substantial threat to the cyber-dependant forces of today. North Korea has made somewhat similar progress and now possesses an extremely complex IADS with strong C2 ability. Forces in Iraq and Afghanistan have experienced an industrious and improvising foe. Our forces, however, must maintain the support and enthusiasm to face these new challenges and develop the capabilities required to act freely in the air, on the sea, on the land, in space, and in the transcendent domain, *cyberspace.*

To be capable to fly, flight and win in cyberspace is to ensure freedom of action. Our potential enemies will work to deny our abilities in the traditional domains. As discussed, laser communication technologies have marked advantages over traditional systems. The need to develop this technology is evident in the ever-growing omnipresence of the threats that exist and will exist in the future. The doctrine and vision of our armed forces currently reflects responses that work to address those threats. In the future, strategic guidance will adapt to the emerging threats, as will the need to update doctrinal response and the training and equipping of forces to meet and anticipate the needs. In order to provide commanders at all levels and provide "… future Presidents with an expanded set of options to address … focus areas and a wide range of potential future contingencies …"[55] we must explore new technologies to fly, fight and win in cyberspace. We cannot wait until potential adversaries have the capability to deny our freedom of action. The advantages of laser technology should be further researched, developed, tested and incorporated in order to provide sequenced, synchronized and deconflicted freedom of action in the form of navigation, verbal, non-verbal and datalink communications and weapons employment capabilities to warfighters at all levels in the *battlefield* that has and will continue to become an extremely technologically-reliant, innovative and cyber-intensive *battle-space.*

Recommendation – The Way Forward

The way forward is to conceptualize and anticipate future needs. To provide the chain of command from the POTUS on down to the individual unit commander the "expanded set of options of options to address … a wide range of potential future contingencies"[56] is to continue to push development of advanced technologies that provide the warfighter with an edge on the battlefield. Civilian, commercial and military contractors and service-members must continue to be further challenged to produce the technologies required to provide the basic capabilities to aviate, navigate and communicate on the battle-space of today and anticipate the needs of tomorrow. To do so, the development of laser-based technologies should be strongly considered as a path to fly, fight and win in the air, on land, sea, in space and in cyberspace.

Suggested Additional Readings

Though not specifically cited in this research paper, additional insight into some of the topics addressed can be found in the below publications and writings concerning operational doctrine, laser technological capabilities and limitations, and potential adversary capabilities.

Air Force Doctrine Document (AFDD) 2-2.1. *Counterspace Operations.* 2 August 2004.

Air Force Doctrine Document (AFDD) 2-5. *Information Operations.* 11 January 2005.

Air Force Doctrine Document (AFDD) 2-5.2. *Intelligence, Surveillance and Reconnaissance Operations.* 21 April 1999.

Air Force Doctrine Document (AFDD) 2-11 v1.4 (Final). *Cyberspace Operations.* 31 November 2008.

Air Force Instruction 33-115, Volume 1. *Network Operations (NetOps).* 24 May 2006.

Alexander, Lt Gen Keith B. "Warfighting in Cyberspace." *Joint Forces Quarterly,* Issue 46, 3rd Quarter (2007).

Chandler, Gen Howie. "An Airman's Perspective: Air, Space and Cyberspace Strategy for the Pacific." *Strategic Studies Quarterly*, Volume 2, Number 2 (Summer 2008).

Covertino, Sebastian M., III, Lou And Demattei and Tammy M. Knierim. *Flying and Fighting in Cyberspace.* Maxwell AFB, AL: Air University Press, July 2007.

Crane, Conrad C. *American Air Power Strategy in Korea 1950-1953.* Lawrence, KS: University Press of Kansas, 2000.

Croom, Charles E., Jr.. "Cyberspace Global Network Operations." *Joint Forces Quarterly,* Issue 46, 3rd Quarter (2007).

Department of Defense Office of Force Transformation. *The Implementation of Network-Centric Wafare.* Washington, DC. 5 January 2005.

Elder, Gen Robert J. "Global and Theater Operations Integration." *Joint Forces Quarterly,* Issue 46, 3rd Quarter (2007).

Henderson, Scott J. *The Dark Visitor: Inside the World of Chinese Hackers.* Fort Leavenworth, KS: Foreign Military Studies Office, 2007.

Huber, Arthur F., Gary Carlberg, Prince Gilliard and David L. Marquet. "Deconflicting Electronic Warfare in Joint Operations." *Joint Forces Quarterly*, Issue 45, 2nd Quarter (2007).

Joint Publication (JP) 3-0. *Joint Operations*. 17 September 2006, incorporating Change 1, 13 February 2008.

Joint Publication (JP) 3-13. *Information Operations.* 13 February 2006.

Joint Publication (JP) 5-0. *Joint Operation Planning.* 26 December 2006.

Joint Publication (JP) 6-0. *Joint Communications System.* 20 March 2006.

Joint Staff, Command, Control, Communications and Computers Directorate (J-6). *Joint Net-Centric Operations Campaign Plan.* October 2006.

Liang, Qiao and Wang Xiangsui. *Unrestricted Warfare.* Beijing: PLA Literature and Arts Publishing House, February 1999.

Lord, Carnes. "On the Nature of Strategic Communications." *Joint Forces Quarterly*, Issue 46, 3rd Quarter (2007).

Lord, Maj Gen William T.. "USAF Cyberspace Command: To Fly and Fight in Cyberspace." *Strategic Studies Quarterly,* Volume 2, Number 3 (Fall 2008).

Matthews, William. "Security Experts: Cyberattacks Will Increase." *Air Force Times.* Army Times Publishing Company, 4 November 2008. http://www.airforcetimes.com/news/2008/11/airforce_cyberattacks_1104008/ (accessed 01 February 2009).

Office of the Secretary of Defense. *Military Power of the People's Republic of China 2007.* Washington, DC. 2007.

Stephens, Hampton. "War in the Third Domain," *AFA Magazine,* April 2007.

Weisgerber, Marcus. "Cyber Operations Could Disrupt, Delay, Deny Air Force Missions." *Air Force Aimpoints,* 29 May 2007. http://aimpoints.hq.af.mil/display.cfm?id=18926 (accessed 05 July 2008).

Glossary

ABCC	Airborne Battlefield Command and Control
AFDD	Air Force Doctrine Document
AOR	Area of Operation
ASAT	Anti-Satellite
C2	Command and Control
C4I	Command, Control, Computers, Communications and Intelligence
C4ISR	Command, Control, Computer, Communications, Intelligence, Surveillance, and Reconnaissance
CAOC	Combined Air Operations Center
CAS	Close Air Support
CDE	Collateral Damage Estimate
CEC	Cooperative Engagement Capability
CEP	Circular Error Probability
CJCS	Chairman of the Joint Chiefs of Staff
CNO	Chief of Naval Operations
COCOM	Combatant Commander
COP	Common Operating Picture
CSAF	Chief of Staff of the Air Force
CSG	Carrier Strike Group
DARPA	Defense Advanced Research Projects Agency
DDoS	Distributed Denial of Service
DHS	Department of Homeland Security
DOD	Department of Defense
DON	Department of the Navy
DTIC	Defense Technical Information Center
EHF	Extremely High Frequency
EMI	Electromagnetic Interference
EMP	Electromagnetic Pulse
FAC	Forward Air Controller
FAC(A)	Forward Air Controller (Airborne)
FSOC	Free-Space Optical Communications
FM	Army Field Manual
FM	Frequency Modulation
GCC	Geographic Combatant Commander
GIG	Global Information Grid
GIOVE-A	Galileo In-Orbit Validation Element-A
HF	High Frequency
IADS	Integrated Air Defense Systems
INS	Inertial Navigation System
IO	Information Operations
IR	Infrared
ISR	Intelligence, Surveillance and Reconnaissance
JCS	Joint Chiefs of Staff

JFC	Joint Force Commander
JP	Joint Publication
JPL	Jet Propulsion Lab
JTAC	Joint Tactical Air Controller
LADAR	Laser Detection and Ranging
LASER	Light Amplification by the Stimulated Emission of Radiation
LEO	Low Earth Orbit
LOS	Line-of-Sight
MILSATCOM	Military Satellite Communications
MIT/LL	Massachusetts Institute of Technology/Lincoln Laboratory
NASA	National Aeronautics and Space Administration
NDS	National Defense Strategy of the United States of America
NMS	National Military Strategy of the United States of America
NOAA	National Oceanic and Atmospheric Administration
NRL	Naval Research Laboratory
NRO	National Reconnaissance Office
NSS	National Security Strategy of the United States of America
NSSC	National Strategy to Secure Cyberspace
NWP	Naval Warfare Publication
OTM/ATH	On the Move/At the Halt
PDD	Personal Data Device
PLA	People's Liberation Army
POTUS	President of the United States of America
QDR	Quadrennial Defense Review
QRM	Quadrennial Roles and Missions Review Report
ROVER	Remote Operated Video Enhanced Receiver
RVSM	Reduced Vertical Separation Mumimums
SAT	Satellite
SDDC	Surface Deployment and Distribution Command
SECDEF	Secretary of Defense
SHF	Super High Frequency
SIAP	Single Integrated Air Picture
SOF	Special Operations Forces
TACAN	Tactical Air Navigation
TACP	Tactical Air Control Party
TSAT	Transformational Satellite Communications System
TTP	Tactics, Techniques and Procedures
UAV	Unmanned Aerial Vehicle
UHV	Ultra High Frequency
US	United States
UV	Ultraviolet
VHF	Very High Frequency
VLF	Very Low Frequency
VOR	VHF Omni-directional Radio Range

Bibliography

AOptix Technologies. "Commercial Lasercom." http://www.aoptix.com/commercial_lasercom.html/ (accessed 01 February 2009).

AOptix Technologies. "Defense Lasercom." http://www.aoptix.com/defense_lasercom.html/ (accessed 01 February 2009).

Armistead, Leigh. *Information Operations: Warfare and the Hard Reality of Soft Power.* Washington, DC: Brassey's, Inc., 2004.

ARRL. "Laser Communications." American Radio Relay League. http://www.arrl.org/tis/info/laser/html (accessed 24 November 2008).

Aviation Week. "Defense Officials Raise ASAT Concerns." *Aviation Week.* The McGraw-Hill Companies. http://www.aviationweek.com/aw/generic/story_channel.jsp?channel=space&id=news/asat032807.xml (accessed 31 January 2009).

Berger, Brian. "NASA to Test Laser Communications with Mars Spacecraft." *Space News.* Imaginova Trade Publishing. http://www.space.com/spacenews/businessmonday_0411115.html (accessed 24 November 2008).

Boeing Laser Communications Demonstration Validates a Critical Element of TSAT Network. Boeing IDS Communications. http://www.boeing.com/ids/news/2006/q3/060801a_nr.html (accessed 24 November 2008).

Brown, Maj. "Working For 'The Man': FAC(A) Coordination for Ground Commanders." *Air Land Sea Bulletin,* Issue No. 2009-1 (January 2009).

Cameron, Alan. "The System – Jammer Location Gets NGA Attention." GPS World. 1 July 2008. http://sidt.gpsworld.com/gpssidt/The+System/The-System-mdash-Jammer-Location-Gets-NGA-Attentio/ArticleStandard/Article/Detail/525881/ (accessed 01 February 2009).

Carter, Kieth and Michael Muccio. "Laser Communications System." Cornell. 2003. http://instruct1.cit.cornell.edu/ee476/FinalProjects/s2003/kmc29/index.htm (accessed 24 November 2008).

Chairman of the Joint Chiefs of Staff. *National Military Strategy of the United States of America: A Strategy for Today; A Vision for Tomorrow.* Washington, DC. 2004.

Grossberg, Adam and Denise Panyik-Dale. *Lucent Technologies Awarded Two Contracts Valued at $26 Million by United States' Department of Defense.* Alcatel-Lucent. Murray Hill, NJ: 21 April 2004. http://www.alcatel-lucent.com/wps/portal/NewsReleases/DetailLucent?MSG_CABINET=Docs_and_Resource_Ctr&MSG_CONTENT_FILE=News_Releases_LU_2004/LU_NEWS_ARTICLE_005031.xml (accessed 24 November 2008).

Hemmati, Hamid. *Overview: Free-Space Optical Communications at JPL/NASA.* Optical Communications Group, JPL. Pasadena, CA: March 2003. http://lasers.jpl.nasa.gov/PAGES/pubs.html#recent (accessed 24 November 2008).

Joint Publication (JP) 3-01. *Countering Air and Missile Threats.* 05 February 2007.

Kenyon, Henry S. "Lasers Detect Targets From the Sky." *SIGNAL Online Magazine.* Armed Forces and Communications Association. December 2006.

http://www.afcea.org/signal/articles/templates/Signal_Article_Template.asp?articleid=1233 (accessed 05 February 2009).
Lander, Mark, John Markoff and Steven Lee. "Digital Fears Emerge After Data Siege in Estonia." *The New York Times.* The New York Times Company, NY: 29 May 2007. http://www.nytimes.com/2007/05/29/technology/29estonia.html?pagewanted=1&_r=1 (accessed 01 February 2009).
Lawler, Maryann. "Lasers Target Covert Communications." *SIGNAL Online Magazine.* Armed Forces and Communications Association. November 2008. http://www.afcea.org/signal/articles/anmviewer.asp?a=1747&print=yes (accessed 05 February 2009).
McLaughlin, Scott and Daniel Wolfe. "A New ETL 449 MHz Wind Profiler for TARS." NOAA Environmental Technology Laboratory. Boulder, CO: NOAA R/ETT77, 04 February 2002. http://www.etl.noaa.gov/technology/tars/ (accessed 27 February 2009).
MSNBC. "Navy Says Missile Smashed Wayward Satellite." MSNBC. https://www.msnbc.com/id/23265613/ (accessed 31 January 2009).
Newswise. "Cracking the Secret Code of Europe's Galileo Satellite." http://www.newswise.com/p/articles/view/521790/ 07 July 2006 (accessed 03 February 2009).
Office of the President of the United States. *The National Security Strategy of the United States of America.* Washington, DC. March 2006.
Office of the President of the United States. *The National Strategy to Secure Cyberspace.* Washington, DC. February 2003.
Office of the Secretary of Defense. *Quadrennial Defense Review Report.* Washington, DC. February 2006.
Ibid. *Quadrennial Roles and Missions Review Report.* Washington, DC. January 2009.
Ott, Lt Col William J., and SMSgt Christopher A. Davis. "Digitally-aided CAS Grows Roots in Theater Operations." *Air Land Sea Bulletin,* Issue No. 2009-1 (January 2009).
Scobell, Andrew. *China's Use of Military Force: Beyond the Great Wall and the Long March.* New York, NY: Cambridge University Press, 2003.
Singer, Jeremy. "U.S.-Led Forces Destroy GPS Jamming Systems in Iraq." *Space News.* 25 March 2003. http://www.space.com/news/gps_iraq_030325.html/ (accessed 27 February 2009).
Singer, Jeremy. "War In Iraq Boosts Case For More Jam Resistant GPS." *Space News.* 08 April 2003. http://www.space.com/spacenews/archive03/gpsarch_040703.html/ (accessed 01 February 2009).
Swanson, E. A. and R. S. Bondurant. *A Space-based Optical Communication System Utilizing Fiber Optics.* Massachusetts Institute of Technology Lincoln Laboratory. Lexington, MA: 9 November 1989.
Thomas, Timothy L. *Cyber Silhouettes: Shadows Over Information Operations.* Fort Leavenworth, KS: Foreign Military Studies Office, 2005.
Ibid. *Dragon Bytes: Chinese Information-War Theory and Practice from 1995-2003.* Fort Leavenworth, KS: Foreign Military Studies Office, 2004.
U.S. Department of Commerce, National Telecommunications and Information Administration, Office of Spectrum Management. "United States Frequency Allocations – The Radio Spectrum." U.S. Department of Commerce. October 2003.

Vice Chairman of the Joint Chiefs of Staff. "Definition of Cyberspace Operations." Washington, DC. 29 September 2008.
Wescher, Matthew. "How Lasers Work." 01 April 2000. http://science.howstuffworks.com/laser.htm/ (accessed 04 February 2009).

Endnotes

[1] U.S. Department of Commerce, *United States Frequency Allocations – The Radio Spectrum.*
[2] Hemmati, *Overview: Free-Space Optical Communications*, 2. Graphic reconstructed from original for clarity.
[3] Office of the President of the United States. *The National Security Strategy of the United States of America*, i.
[4] Ibid, 22.
[5] Ibid, 43-44.
[6] Office of the Secretary of Defense, *Quadrennial Defense Review Report*, viii.
[7] Ibid, 30-32.
[8] Chairman of the Joint Chiefs of Staff, *National Military Strategy of the United States of America*, iii.
[9] Ibid, 3.
[10] Ibid, 5.
[11] Ibid, 15-16.
[12] Office of the President of the United States, *The National Strategy to Secure Cyberspace*, 49-50.
[13] JP 3-01, *Countering Air and Missile Threats*, I-6-7.
[14] Aviation Week, *Defense Officials Raise ASAT Concerns.*
[15] Ibid.
[16] MSNBC, *Navy Says Missile Smashed Wayward Satellite.*
[17] Scobell, *China's Use of Military Force,* 190.
[18] Thomas, *Cyber Silhouettes*, 283-284.
[19] Armistead, *Information Operations*, 211.
[20] Thomas, *Dragon Bytes*, 61.
[21] Lander et al, *Digital Fears Emerge After Data Siege in Estonia.*
[22] Ibid, and Office of the President of the United States, *The National Strategy to Secure Cyberspace*, 50.
[23] Williams, *Security Experts: Cyberattacks Will Increase.*
[24] Singer, *War in Iraq Boosts Case For More Jam Resistant GPS.*
[25] Cameron, *The System.*
[26] Brown, *Working For 'The Man,'* and Ott and Davis, *Digitally-aided CAS Grows Roots in Theater Operations.*
[27] Newswise, *Cracking The Secret Codes of Europe's Galileo Satellite.*
[28] Ibid.
[29] Singer, *U.S.-Led Forces Destroy GPS Jamming Systems in Iraq.*
[30] Wescher, *How Lasers Work.*
[31] Ibid.
[32] Ibid.
[33] Ibid.
[34] U.S. Department of Commerce, *United States Frequency Allocations – The Radio Spectrum.*
[35] Ibid.
[36] ARRL, *Laser Communications*, 19.
[37] Grossberg, *Lucent Technologies;* and Boeing IDS Communications, *Boeing Laser Communications.*
[38] Swanson, *A Space-based Optical Communication System Utilizing Fiber Optics.*
[39] Berger, *NASA to Test Laser Communications with Mars Spacecraft.*
[40] Ibid.
[41] Boeing IDS Communications, *Boeing Laser Communications.*
[42] Grossberg, *Lucent Technologies.*
[43] Ibid.
[44] Lawlor, *Lasers Target Covert Communications.*
[45] Kenyon, *Lasers Detect Targets From the Sky.*
[46] AOptix Technologies, *Commercial Lasercomm*, and *Defense Lasercomm.*
[47] Berger, *NASA to Test Laser Communications with Mars Spacecraft;* and Kenyon, *Lasers Detect Targets From the Sky*; and Lawlor, *Lasers Target Covert Communications.*
[48] Ibid.
[49] Hemmati, *Overview: Free-Space Optical Communications*, 2.
[50] Ibid. Graphic reconstructed from original for clarity.
[51] Mclaughlin and Wolfe, *A New ETL 449 MHz Wind Profiler for TARS.*

[52] Carter and Muccio, *Laser Communications System.*
[53] Vice Chairman of the Joint Chiefs of Staff, *Definition of the Cyberspace Operations.*
[54] Office of the Secretary of Defense, *Quadrennial Roles and Missions Review Report,* 14.
[55] Ibid, *Quadrennial Defense Review Report*, 30-32.
[56] Ibid, viii.